



## PATENT ABSTRACTS OF JAPAN

(11) Publication number: **09097216 A**(43) Date of publication of application: **08.04.97**

(51) Int. Cl.

**G06F 12/14**  
**G09C 1/00**  
**G09C 1/00**  
**G11B 20/10**  
**G11B 20/12**  
**H04L 9/08**

(21) Application number: **08098950**(22) Date of filing: **19.04.96**(30) Priority: **25.07.95 JP 07189309**(71) Applicant: **SONY CORP**

(72) Inventor: **OSAWA YOSHITOMO**  
**SAKO YOICHIRO**  
**KURIHARA AKIRA**  
**KAWASHIMA ISAO**

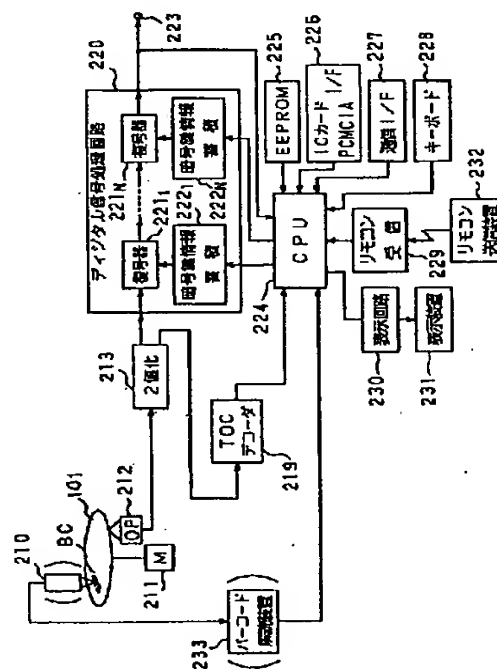
(54) **SIGNAL RECORDING DEVICE, SIGNAL  
 RECORDING MEDIUM AND SIGNAL  
 REPRODUCING DEVICE**

## (57) Abstract:

**PROBLEM TO BE SOLVED:** To make it difficult to perform illegal decode or illegal copy.

**SOLUTION:** This signal reproducing device reproduces enciphered data from a digital recording medium 101 recording the enciphered data, to which one enciphering processing has been performed at least, and key storage place information instructing for the place to arrange one piece of key information for deciphering at least, and this device is provided with a reproducing head device 212 for reading the enciphered data and key storage place information from the recording medium 101, TOC decoder 219, CPU 224 or the like and a digital signal processing circuit 220 for deciphering the enciphered data by using the key information of the place designated based on the key storage place information.

COPYRIGHT: (C)1997,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-97216

(43) 公開日 平成9年(1997)4月8日

(51) Int. Cl. <sup>8</sup>	識別記号	序内整理番号	F I	技術表示箇所
G 0 6 F 12/14	3 2 0		G 0 6 F 12/14	3 2 0 B
G 0 9 C 1/00	6 3 0	7259-5J	G 0 9 C 1/00	6 3 0 A
	6 6 0	7259-5J		6 6 0 D
G 1 1 B 20/10		7736-5D	G 1 1 B 20/10	H
20/12	1 0 2	9295-5D	20/12	1 0 2
審査請求 未請求 請求項の数11 O L (全 25 頁) 最終頁に続く				

(21) 出願番号 特願平8-98950

(22) 出願日 平成8年(1996)4月19日

(31) 優先権主張番号 特願平7-189309

(32) 優先日 平7(1995)7月25日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 大塚 義知

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72) 発明者 佐古 曜一郎

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72) 発明者 栗原 章

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 弁理士 小池 晃 (外2名)

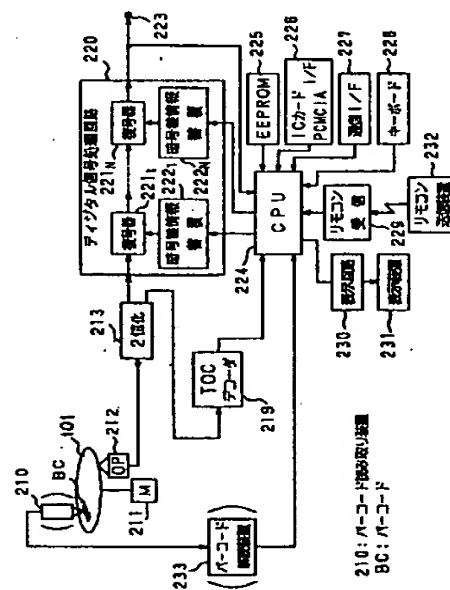
最終頁に続く

(54) 【発明の名称】 信号記録装置、信号記録媒体、及び信号再生装置

(57) 【要約】

【課題】 不法解読や不法コピーの防止を困難にする。

【解決手段】 少なくとも一つの暗号化処理が施された暗号化されたデータと、当該暗号化を解くための少なくとも一つの鍵情報が配置される場所を指示する鍵格納場所情報とが記録されてなるデジタル状記録媒体101から暗号化データを再生する信号再生装置であり、記録媒体101から暗号化データと鍵格納場所情報を読み取る再生ヘッド装置12、TOCデコーダ219、及びCPU224等と、鍵格納場所情報に基づいて指定された場所の鍵情報を用いて、暗号化データを復号化するデジタル信号処理回路220とを有する。



## 【特許請求の範囲】

【請求項1】 信号記録媒体に対して暗号化した信号を記録する信号記録装置において、

入力信号を暗号化する少なくとも一つの信号暗号化手段と、

上記少なくとも一つの信号暗号化手段にて使用する暗号化の鍵情報が配置される場所を指示する鍵格納場所情報を入力する鍵格納場所情報入力手段とを有することを特徴とする信号記録装置。

【請求項2】 上記鍵格納場所情報を信号記録媒体のユーザがアクセスできない特定の位置に記録することを特徴とする請求項1記載の信号記録装置。

【請求項3】 上記鍵情報を、信号記録媒体上又は当該信号記録媒体以外の場所に配置することを特徴とする請求項1記載の信号記録装置。

【請求項4】 上記鍵情報を暗号化する鍵情報暗号化手段と、上記鍵情報暗号化手段にて使用する暗号化の鍵情報が配置される場所を指示する格納情報指示情報を入力する格納情報指示情報入力手段とを、設けることを特徴とする請求項1記載の信号記録装置。

【請求項5】 少なくとも一つの暗号化処理が施された暗号化信号と、当該暗号化信号の暗号化を解くための少なくとも一つの鍵情報が配置される場所を指示する鍵格納場所情報とが記録されてなることを特徴とする信号記録媒体。

【請求項6】 上記鍵格納場所情報が記録される位置は、ユーザがアクセスできない特定の位置であることを特徴とする請求項5記載の信号記録媒体。

【請求項7】 上記鍵格納場所情報は暗号化されており、当該鍵格納場所情報の暗号化の鍵情報をも記録してなることを特徴とする請求項5記載の信号記録媒体。

【請求項8】 少なくとも一つの暗号化処理が施された暗号化信号と、当該暗号化信号の暗号化を解くための少なくとも一つの鍵情報が配置される場所を指示する鍵格納場所情報とが記録されてなる信号記録媒体から上記暗号化信号を再生する信号再生装置であって、

上記信号記録媒体から上記暗号化信号及び上記鍵格納場所情報を読み取る読み取り手段と、

上記鍵格納場所情報に基づいて指定された場所の上記鍵情報を用いて、上記暗号化信号の当該暗号化を解く復号手段とを有することを特徴とする信号再生装置。

【請求項9】 上記読み取り手段は、信号記録媒体のユーザがアクセスできない特定の位置に記録された上記鍵格納場所情報を読み取ることを特徴とする請求項8記載の信号再生装置。

【請求項10】 信号記録媒体以外の場所に配置された上記鍵情報を取り出す取り出し手段を備えることを特徴とする請求項8記載の信号再生装置。

【請求項11】 上記鍵情報は暗号化されており、上記読み取り手段は、当該鍵情報の暗号化の鍵情報が配置さ

れる場所を指示する情報をも読み取ることを特徴とする請求項8記載の信号再生装置。

## 【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コピーの防止や不正使用を阻止するための信号記録装置、信号記録媒体、及び信号再生装置に関する。

【0002】

【従来の技術】近年において、光ディスク等の信号記録媒体の大容量化と普及により、記録されている信号の著作権を保護するために、不法なコピーの防止が重要とされていきている。すなわち、デジタルオーディオデータやデジタルビデオデータの場合には、コピー或いはダビングにより劣化の無い複製物を容易に生成でき、またコンピュータデータの場合には、元のデータと同一のデータが容易にコピーできるため、既に不法コピーによる著作権の侵害等の弊害が生じてきているのが実情である。

【0003】このようなことから、上記不法コピーの防止を目的として、オリジナルの信号記録媒体に不法コピー防止のための所定のIDビットを記録しているものがある。

【0004】例えば、いわゆるR-DAT (Rotary head Digital Audio Taperecoder) と称されるデジタルオーディオ信号記録再生装置における上記不法コピー防止のための方式としては、信号記録媒体としてのデジタルオーディオテープ上に記録されるデジタルオーディオ信号のメインデータエリアに、デジタルコピーの禁止や段階的な世代コピーを禁止 (すなわち世代制限) するための禁止コード (いわゆるSCMS: シリアルコピー管理システムの規格の禁止コード) を記録しておき、デジタルオーディオ信号記録装置がこの禁止コードを検出したときに、新たなデジタルオーディオテープ上への当該デジタルオーディオ信号のコピー記録を禁止するような方式が採用されている。

【0005】また、信号記録媒体に記録された例えばデジタルビデオ信号の不法コピーを防止するためには、上記R-DATにおける記録再生装置間での不法コピー防止の方式と同様に、オリジナルのデジタル記録媒体に不法コピー防止のための所定のIDビット (CGMS: コピー世代管理システムの規格の禁止コード) を記録することが考えられる。

【0006】さらに、コンピュータデータの場合には、ファイル内容自体を暗号化鍵情報を用いて暗号化し、それを正規の登録された使用者にのみ使用許諾することが行われている。なおこれは、情報流通の形態として、情報が暗号化されて記録されたデジタル記録媒体を配布しておき、使用者が必要とした内容について料金を払って鍵情報入手し、暗号を解いて利用可能とするようなシステムに結び付くものである。

## 【0007】

【発明が解決しようとする課題】ところが、上述したような従来の信号記録媒体用の禁止コードや暗号鍵情報は、特開平5-173891号公報に示されるように、記録媒体上のユーザからアクセスされるシステム固有の特定の場所に記録されている。なお、上記禁止コードや暗号鍵情報も、通常暗号化されている。

【0008】このように、上記禁止コードや暗号鍵情報の配置がそれぞれの暗号化手法において任意の場所で固定的であると、互換性がなくなる虞れがある。また、禁止コードや暗号鍵情報を固定的に配置すれば、暗号化の手法も固定化されることになり、柔軟性、拡張性に乏しく、フォーマット自身の寿命を縮めてしまう可能性がある。

【0009】さらに、暗号鍵情報や禁止コードは、例えばユーザからアクセス可能な場所にあるため、悪意のあるユーザによる解読や不法コピーの対象になりやすかった。

【0010】そこで、本発明は上述したような実情に鑑みてなされたものであり、不法解読や不法コピーを困難にする信号記録装置及び信号再生装置、並びに信号記録媒体を提供することを目的とする。

## 【0011】

【課題を解決するための手段】本発明の信号記録装置及び信号記録媒体は、入力信号を暗号化した暗号化信号と、当該暗号化の鍵情報が配置される場所を指示する鍵格納場所情報とを信号記録媒体に記録することにより、上述の課題を解決する。

【0012】また、本発明の信号再生装置は、本発明の信号記録媒体から信号を再生するにあたって、当該信号記録媒体から暗号化信号及び鍵格納場所情報を読み取り、鍵格納場所情報に基づいて指定された場所の鍵情報を用いて、暗号化信号を復号することにより、上述の課題を解決する。

【0013】すなわち、本発明によれば、信号記録媒体には鍵情報の場所を指示する鍵格納場所情報を記録し、信号再生の際には当該鍵格納場所情報に基づいて鍵情報を取り出すようにすることで、鍵情報を容易に取り出せないようにしている。

## 【0014】

【発明の実施の形態】以下、本発明に係るいくつかの好ましい実施の形態について、図面を参照しながら説明する。

【0015】図1は、本発明の実施の形態となる信号記録装置の一構成例を概略的に示すブロック図である。この図1において、入力端子11には、例えばアナログのオーディオ信号やビデオ信号をデジタル変換して得られたデータやコンピュータデータ等のデジタルデータが供給されている。この入力デジタルデータは、インターフェース回路12を介して、セクタ化回路13に送

られ、所定データ量単位、例えば2048バイト単位でセクタ化される。

【0016】このセクタ化されたデータは、スクランブル処理回路14に送られてスクランブル処理が施される。この場合のスクランブル処理は、同一バイトパターンが連続して表れないように、すなわち同一パターンが除去されるように、入力データをランダム化して、信号を適切に読み書きできるようにすることを主旨としたランダム化処理のことである。

10 【0017】上記スクランブル処理あるいはランダム化処理されたデータは、ヘッダ付加回路15に送られて、各セクタの先頭に配置されるヘッダデータが付加された後、誤り訂正符号化回路16に送られる。

【0018】次に誤り訂正符号化回路16では、データ遅延及びパリティ計算を行ってパリティを付加する。

【0019】次の変調回路17では、所定の変調方式に従って、例えば8ビットデータを16チャンネルビットの変調データに変換し、同期付加回路18に送る。同期付加回路18では、上記所定の変調方式の変調規則を破

20 る、いわゆるアウトオブブルーのパターンの同期信号を所定のデータ量単位で付加し、駆動回路すなわちドライバ19を介して記録ヘッド20に送っている。

【0020】記録ヘッド20は、例えば光学的あるいは磁気光学的な記録を行うものであり、ディスク状の記録媒体21に上記変調された記録信号の記録を行う。このディスク状記録媒体21は、スピンドルモータ22により回転駆動される。

【0021】なお、上記スクランブル処理回路14は、必須ではなく、また、ヘッダ付加回路15の後段に挿入して、ヘッダ付加されたデジタルデータに対してスクランブル処理を施して誤り訂正符号化回路16に送るようにしてもよい。

【0022】ここで、セクタ化回路13、スクランブル

40 処理回路14、ヘッダ付加回路15、誤り訂正符号化回路16、変調回路17、及び同期付加回路18のいずれか少なくとも1つの回路は、入力に対して暗号化処理を施して出力するような構成を有している。好ましくは、2つ以上の回路で暗号化処理を施すことが挙げられる。

【0023】この暗号化処理の鍵情報は、例えば媒体固有の識別情報、媒体の出荷先の地域を表す仕向け情報 (Regional Code) や、製造元識別情報、販売者識別情報、あるいは、記録装置やエンコーダの固有の識別情報、カッティングマシンやスタンパ等の媒体製造装置の固有の識別情報、外部から供給される識別情報等を少なくとも一部に用いることができるものである。上記回路13～18の少なくとも1つ、好ましくは2以上で当該鍵情報を用いた入力データに対する暗号化処理が施される。

50 【0024】この場合、回路13～18のどの回路において暗号化処理が施されたかも選択肢の1つとなってお

り、再生時に正常な再生信号を得るために必要な鍵と考えられる。すなわち、1つの回路で暗号化処理が施されていれば、6つの選択肢の1つを選ぶことが必要となり、2つの回路で暗号化処理が施されていれば、2つの回路の組み合わせの数に相当する15個の選択肢の内から1つを選ぶことが必要となる。6つの回路13~18の内の1~6つの回路で暗号化処理が施される可能性がある場合には、さらに選択肢が増大し、この組み合わせを試行錯誤的に見つけることは困難であり、充分に暗号の役割を果たすものである。

【0025】さらに、暗号化の鍵情報を所定タイミング、例えばセクタ周期で切り換えることが挙げられる。この所定タイミングで鍵情報の切り換える場合に、切り換えを行うか否かや、切換周期、複数の鍵情報の切換順序等の情報も鍵として用いることができ、暗号化のレベルあるいは暗号の難易度、解き難さ、解読の困難さをさらに高めることができる。

【0026】また、上述した鍵情報は、後述する暗号鍵格納場所情報により指示される媒体101上の位置、或いは当該媒体101上以外の位置に格納されるものである。上記鍵格納場所情報は、例えば上記インターフェース回路12からTOC (Table of contents) 生成回路23を介して端子24に送られる情報であり、また、インターフェース回路12から直接的に端子25に送られる情報である。これらの端子24、25からの鍵格納場所情報が、記録媒体101の例えば後述するTOC領域、或いはその他の所定位置に記録されるようになされている。なお、以下の説明では、TOC領域に鍵格納場所情報が記録される場合を例に挙げている。

【0027】次に、各回路13~18の構成及び暗号化処理の具体例について説明する。

【0028】まず、セクタ化回路13においては、例えば図2に示すような偶数・奇数バイトのインターリーブ処理を行わせることが挙げられる。すなわち、図2において、上記図1のインターフェース回路12からの出力を、2出力の切換スイッチ31に送り、この切換スイッチ31の一方の出力を偶奇インターリーブ33を介してセクタ化器34に送り、切換スイッチ31の他方の出力をそのままセクタ化器34に送っている。セクタ化器34では、例えば入力データの2048バイト単位でまとめて1セクタとしている。このセクタ化回路13の切換スイッチ32の切換動作を、鍵となる1ビットの制御信号で制御するわけである。偶奇インターリーブ33は、図3のAに示すような偶数バイト36aと奇数バイト36bとが交互に配置された入力データの1セクタ分を、図3のBに示すように、偶数データ部37aと奇数データ部37bとに分配して出力する。さらに、図3のCに示すように、1セクタ内の所定の領域39を鍵情報により特定し、この領域39内のデータについてのみ偶数データ部39aと奇数データ部39bとに分配するように

してもよい。この場合には、領域39の特定の仕方を選択通り選択できるように設定することもでき、鍵情報の選択肢をさらに増加させて暗号化のレベルをより高めることもできる。

【0029】次に、スクランブル処理回路14には、例えば図4に示すように、15ビットのシフトレジスタを用いたいわゆるパラレルブロック同期タイプのスクランブラを用いることができる。このスクランブラのデータ入力用の端子35には、LSB (最下位ビット) が時間的に先となる順序、いわゆるLSBファーストで、上記セクタ化回路13からのデータが入力される。スクランブル用の15ビットのシフトレジスタ14aは、排他的論理和 (ExOR) 回路14bを用いて生成多項式  $x^{15} + x + 1$  に従ったフィードバックがかけられ、15ビットのシフトレジスタ14aには、図5に示すようなプリセット値 (あるいは初期値) が設定されるようになっており、図5のプリセット値の選択番号は、例えばセクタアドレスの下位側4ビットの値に対応させて、セクタ単位でプリセット値が切り換えられるようになっている。シフトレジスタ14aからの出力データと端子35からの入力データとは、ExOR回路14cにより排他的論理和がとられて、端子14dより取り出され、図1のヘッダ付加回路15に送られる。

【0030】ここで、上記生成多項式及びプリセット値 (初期値) を、所定の識別番号等の鍵情報に応じて変化させるようにすることができる。すなわち、上記生成多項式を変化させるには、例えば図6に示すような構成を用いればよい。この図6において、15ビットのシフトレジスタ14aの各ビットからの出力が切換スイッチ14fの各被選択端子に送られ、この切換スイッチ14fは制御端子14gからの例えば4ビットの制御データによって切換制御され、切換スイッチ14fからの出力はExOR回路14bに送られている。このような構成の制御端子14gの制御データを変化させることにより、生成多項式  $x^{15} + x^n + 1$  の  $n$  を変化させることができる。また、上記プリセット値を変化させるには、上記図5のプリセット値テーブルの各プリセット値を、例えば16バイトの識別情報の各バイト値と論理演算することが挙げられる。この場合の識別情報としては、上述したような媒体固有の識別情報、製造元識別情報、販売者識別情報や、記録装置やエンコーダの固有の識別情報、媒体製造装置固有の識別情報、外部から供給される識別情報等、あるいはこれらの組み合わせや他の情報との組み合わせ等を用いることができ、また上記論理演算としては、排他的論理和 (ExOR) や、論理積 (AND)、論理和 (OR)、シフト演算等を使用できる。なお、生成多項式を変化させるための構成は図6の構造に限定されず、シフトレジスタの段数や取り出すタップ数を任意に変更してもよい。

【0031】次に、ヘッダ付加回路15について説明す

る。まず、図7はセクタフォーマットの具体例を示しており、1セクタは、2048バイトのユーザデータ領域41に対して、4バイトの同期領域42と、16バイトのヘッダ領域43と、4バイトの誤り検出符号(EDC)領域44とが付加されて構成されている。誤り検出符号領域44の誤り検出符号は、ユーザデータ領域41及びヘッダ領域43に対して生成される32ビットのCRC符号から成っている。ヘッダ付加回路15での暗号化処理としては、同期いわゆるデータシンクに対して、ヘッダのアドレス及びCRCに対して施すことが挙げられる。

【0032】セクタの同期すなわちデータシンクに対して暗号化処理を施す一例としては、4バイトの同期領域42の各バイトに割り当てられたバイトパターンを、図8の「A」、「B」、「C」、「D」にてそれぞれ表すとき、2ビットの鍵情報を用いて、この4バイトの内容をバイト単位でシフトあるいはローテートすることが挙げられる。すなわち、2ビットの鍵が「0」のとき「ABCD」、「1」のとき「BCDA」、「2」のとき「CDAB」、「3」のとき「DABC」のように切り換えることにより、この鍵が合致しないとセクタの同期がとれなくなり、正常な再生が行えない。なお、上記バイトパターン「A」～「D」としては、例えばISO646のキャラクタコード等を使用できる。

【0033】ヘッダ領域43内には、図9に示すように、いわゆる巡回符号であるCRC45、コピーの許可／不許可やコピー世代管理等のためのコピー情報46、多層ディスクのどの層かを示す層47、アドレス48、予備49の各領域が設けられている。この内で、アドレス48の32ビットにビットスクランブル、この場合には、ビット単位での転置処理を施すことにより、暗号化が行える。また、CRC45の生成多項式として、 $x^{16} + x^{15} + x^2 + 1$  が用いられている場合、第2、第3項の $x^{15}$ 、 $x^2$ の代わりに、 $x^{15} \sim x$ に対応する15ビットを鍵に応じて変化させることが挙げられる。また、CRC45の16ビットと鍵情報とを論理演算することも挙げられる。

【0034】なお、上記鍵情報は、上述したように、媒体固有の識別情報、製造元識別情報、販売者識別情報や、記録装置やエンコーダ、あるいは媒体製造装置の固有の識別情報、外部から供給される識別情報等、あるいはこれらの組み合わせや他の情報との組み合わせ等を用いることができる。

【0035】次に、誤り訂正符号化回路16の具体例を図10に示す。この図10において、誤り訂正符号化の1フレームは148バイトあるいは148シンボルのデータから成り、上記ヘッダ付加回路15からのデジタルデータが148バイト毎にまとめられて、第1の符号化器であるC1エンコーダ52に供給される。C1エンコーダ52では8バイトのPパリティが付加され、イン

ターリーブのための遅延回路53を介して第2の符号化器であるC2エンコーダ54に送られる。C2エンコーダ54では14バイトのQパリティが付加され、このQパリティは遅延回路55を介してC1エンコーダ52に帰還されている。このC1エンコーダ52からのP、Qパリティを含む170バイトが取り出されて、遅延回路56を介し、インバータ部57aを有する再配列回路57を介して出力され、図1の変調回路17に送られる。

【0036】このような誤り訂正符号化回路において暗号化処理を施す場合には、例えば再配列回路57内のインバータ部57aの各バイト毎に、暗号の鍵情報に応じてインバータを入れるか入れないかの選択を行わせるようにすることが挙げられる。すなわち、基準構成においては、22バイトのP、Qパリティに対して再配列回路57のインバータ部57aのインバータによる反転が行われて出力されるが、これらのインバータのいくつかを無くしたり、C1データ側にいくつかのインバータを入れて反転して出力させたりすることが挙げられる。

【0037】このようなデータ変換を施す場合、基準構成からの違いの程度によって誤り訂正不能確率が変化し、違いが少ないときには最終的な再生出力におけるエラー発生確率がやや高くなる程度であるのに対し、違いが多いときには全体的にエラー訂正が行われなくなって殆ど再生できなくなるような状態となる。すなわち、例えばC1エンコーダについて見ると、誤り訂正能力を示す指標であるいわゆるディスタンスが9であるため、最大4バイトまでのエラー検出訂正が行え、消失(イレージャ)ポイントがあれば最大8バイトまでの訂正が可能であることから、違いが5箇所以上あると、C1符号では常に訂正不可又は誤訂正となる。違いが4箇所の場合は、他に1バイトでもエラーが生じると訂正不可という微妙な状態となる。違いが3、2、1箇所と減少するにつれて、誤り訂正できる確率が増えてゆく。これを利用すれば、オーディオやビデオのソフトを提供する場合等に、ある程度は再生できるが完璧ではなく時々乱れる、といった再生状態を積極的に作り出すことができ、該ソフトの概要だけを知らせる用途等に使用することができる。

【0038】この場合、予めインバータの変更を行う場所を例えば2箇所程度規定しておく方法と、変更箇所を鍵情報に応じてランダムに選び、最低個数を2箇所程度に制限する方法と、これらを複合する方法とが挙げられる。

【0039】さらに、インバータの挿入あるいは変更位置としては、図10の再配列回路57の位置に限定されず、例えばC1エンコーダ52の前段や後段等の他の位置やこれらの位置を組み合わせるようにしてもよい。複数の位置の場合に、異なる鍵を用いるようにしてもよい。また、インバータを用いる以外に、ビット加算や種々の論理演算を用いるようにしてもよい。また、シフト

レジスタを用いて変換したり、各種関数演算により変換する等、さまざまな暗号化手法が適用できることは勿論であり、それらを組み合わせて使用することも可能である。

【0040】ここで、図11は、上記誤り訂正符号化回路16の他の具体例として、再配列回路57内のインバータ部57aの後段の位置に排他的論理和(ExOR)回路群61を挿入し、C1エンコーダ52の前段すなわち入力側の位置にもExOR回路群66を挿入した例を示している。

【0041】具体的に、ExOR回路群61は、C1エンコーダ52から遅延回路56、及び上記再配列回路57のインバータ部57aを介して取り出される170バイトのデータ、すなわち情報データC1<sub>170n+169</sub>~C1<sub>170n+22</sub>及びパリティデータP1<sub>170n+21</sub>~P1<sub>170n+14</sub>、Q1<sub>170n+13</sub>~Q1<sub>170n</sub>のデータに対して排他的論理和(ExOR)回路を用いたデータ変換を行い、ExOR回路群66は、148バイトの入力データB<sub>148n</sub>~B<sub>148n+147</sub>に対して排他的論理和(ExOR)回路を用いたデータ変換を行う。これらのExOR回路群61、66に用いられるExOR回路は、1バイトすなわち8ビットの入力データと1ビットの制御データで指示される所定の8ビットデータとの排他的論理和(ExOR)をそれぞれとるような8ビットExOR回路であり、このような8ビットExOR回路(所定の8ビットデータがオール1の場合はインバータ回路に相当する)が、ExOR回路群61では170個、ExOR回路群66では148個用いられている。

【0042】この図11においては、170ビットの鍵情報が端子62に供給され、いわゆるDラッチ回路63を介してExOR回路群61内の170個の各ExOR回路にそれぞれ供給されている。Dラッチ回路63は、イネーブル端子64に供給された1ビットの暗号化制御信号に応じて、端子62からの170ビットの鍵情報をそのままExOR回路群61に送るか、オールゼロ、すなわち170ビットの全てを“0”とするかが切換制御される。ExOR回路群61の170個の各ExOR回路の内、Dラッチ回路63から“0”が送られたExOR回路は、再配列回路57内のインバータ部57aからのデータをそのまま出力し、Dラッチ回路63から“1”が送られたExOR回路は、再配列回路57内のインバータ部57aからのデータを反転して出力する。オールゼロのときには、再配列回路57内のインバータ部57aからのデータをそのまま出力することになる。また、ExOR回路群66については、148個のExOR回路を有し、鍵情報が148ビットであること以外は、上記ExOR回路群61の場合と同様であり、端子67に供給された148ビットの鍵情報がDラッチ回路68を介してExOR回路群66内の148個のExOR回路にそれぞれ送られると共に、Dラッチ回路68はイネーブル端子69の暗号化制御信号により148ビットの鍵情報がオールゼロかが切換制御される。

【0043】この図11の例において、ExOR回路群61は、C1エンコーダ52から遅延回路56、インバータ部57aを介して取り出される170バイトのデータとしての情報データC1<sub>170n+169</sub>~C1<sub>170n+22</sub>及びパリティデータP1<sub>170n+21</sub>~P1<sub>170n+14</sub>、Q1<sub>170n+13</sub>~Q1<sub>170n</sub>のデータに対して排他的論理和(ExOR)回路を用いたデータ変換を行っているが、パリティデータについてはデータ変換を行わず、残り148バイトの情報データC1<sub>170n+169</sub>~C1<sub>170n+22</sub>に対して、148ビットの鍵情報に応じたデータ変換を行わせるようにしてもよい。

【0044】この図11の回路においても、上記図10の場合と同様な作用効果が得られることは勿論である。また、ExOR回路群61、66のいずれか一方のみを使用するようにしたり、いずれか一方あるいは双方の選択も暗号化の鍵として用いるようにすることもできる。

【0045】なお、上記鍵情報は、上述したように、媒体固有の識別情報、製造元識別情報、販売者識別情報や、記録装置やエンコーダあるいは媒体製造装置の固有の識別情報、外部から供給される識別情報等、あるいはこれらの組み合わせや他の情報との組み合わせ等を用いることができる。

【0046】なお、上記データ変換手段としてのExOR回路群61、66の代わりに、AND、OR、NAND、NOR、インバート回路群等を使用してもよい。また、8ビット単位で1ビットの鍵情報あるいは鍵データによる論理演算を行う以外にも、8ビットの情報データに対して8ビットの鍵データで論理演算を行わせてもよく、さらに、情報データの1ワードに相当する8ビットの内の各ビットに対してそれぞれAND、OR、ExOR、NAND、NOR、インバート回路を組み合わせ使用してもよい。この場合には、例えば148バイトすなわち148×8ビットのデータに対して、148×8ビットの鍵データが用いられることになり、さらにAND、OR、ExOR、NAND、NOR、インバート回路を組み合わせ使用する場合には、これらの組み合わせ自体も鍵として用いることができる。また、論理演算以外に、データの位置を変える転置や、データの値を置き換える置換等も上記データ変換として使用できる。また、シフトレジスタを用いて変換したり、各種関数演算により変換する等、さまざまな暗号化手法が適用できることは勿論であり、それらを組み合わせて使用することも可能である。

【0047】次に、図1の変調回路17での暗号化処理について、図12を参照しながら説明する。この図12において、入力端子71には、上記誤り訂正符号化回路16からのデータが8ビット(1バイト)毎に供給され、入力端子72には8ビットの鍵情報が供給されており、これらの8ビットデータは、論理演算回路の一例としてのExOR回路73に送られて排他的論理和がとられ



る。このExOR回路73からの8ビット出力が、所定の変調方式の変調器、例えば8-16変換回路74に送られて、16チャンネルビットに変換される。この8-16変換回路74での8-16変調方式の一例としてはいわゆるEFMプラス変調方式が挙げられる。

【0048】この図12の例では、データ変調の前に8ビットの鍵情報を用いた暗号化処理を施しているが、鍵情報のビット数は8ビットに限定されず、また、8-16変調の際の変換テーブルの入出力の対応関係を鍵情報に応じて変化させるようにしてもよい。鍵情報には、上述した媒体固有の識別情報等を使用できることは勿論である。

【0049】次に、同期付加回路18について説明する。同期付加回路18では、例えば図13に示すような4種類の同期ワードS0~S3を用いて、上記8-16変調のフレーム単位で同期をとっている。この8-16変調フレーム（例えばEFMプラスフレーム）は、例えば85データシンボルである1360チャンネルビットから成り、この1フレーム1360チャンネルビット毎に32チャンネルビットの同期ワードが付加されると共に、このフレームを上記C1符号やC2符号に対応させて構造化し、C1符号系列の先頭フレームの同期ワードと他のフレームの同期ワードを異ならせる等して、上記4種類の同期ワードS0~S3を使い分けている。これらの同期ワードS0~S3は、直前のワードの“1”、“0”の状態やいわゆるデジタルサムあるいは直流値等に応じてそれぞれ2つの同期パターンa、bを有している。

【0050】このような4種類の同期ワードS0~S3の選択を、例えば図14に示すような回路を用いて、2ビットの鍵情報75に応じて変更することにより、暗号化が行える。すなわち、上記4種類の同期ワードS0~S3を指定する2ビットデータ76の各ビットと、上記2ビットの鍵情報75の各ビットとが、2つのExOR回路77、78によりそれぞれ排他的論理和され、新たな同期ワード指定データ79となる。これにより、上記フレーム構造における同期ワードの使い方あるいはフレーム構造内での各種同期ワードの使用位置が変更され、暗号化がなされることになる。

【0051】なお、同期ワードの種類数をさらに増やしてそれらの内から4種類の同期ワードを取り出す取り出し方を暗号化の鍵により決定するようにしてもよい。この鍵情報としては、上述した媒体固有の識別情報等が使用できる。

【0052】次に図15は、記録媒体の一例としての光ディスク等のディスク状記録媒体101を示している。このディスク状記録媒体101は、中央にセンタ孔102を有しており、このディスク状記録媒体101の内周から外周に向かって、プログラム管理領域であるTOC (table of contents) 領域となるリードイン (leadin

) 領域103と、プログラムデータが記録されたプログラム領域104と、プログラム終了領域、いわゆるリードアウト (lead out) 領域105とが形成されている。オーディオ信号やビデオ信号再生用光ディスクにおいては、上記プログラム領域104にオーディオやビデオデータが記録され、このオーディオやビデオデータの時間情報等が上記リードイン領域103で管理される。

【0053】当該図15の記録媒体101において、前記鍵格納場所情報は、リードイン領域103に、TOC情報の一部として記録される。再生時には、上記鍵格納場所情報を読み出し、この読み出した鍵格納場所情報に基づいて、前記暗号化を復号するための鍵情報を取り出すようにする。

【0054】なお、上記鍵格納場所情報にて格納場所が指示される鍵情報の当該格納場所については後述する。

【0055】次に、上記ディスク状記録媒体101からデータを再生する再生装置について、図16を用いて説明する。

【0056】図16において、上記ディスク状記録媒体101は、スピンドルモータ211により回転駆動され、光学ピックアップ装置等の再生ヘッド装置212により当該記録媒体101の記録内容が読み取られる。

【0057】再生ヘッド装置212により読み取られた信号は、2値化回路213にて2値のデジタルデータに変換され、デジタル信号処理回路220に送られる。また、上記2値化回路213にて2値に変換されたデジタルデータのうち、TOC領域から読み出されたデータは、TOCデコーダ219に送られてデコード処理され、このデコード処理により得られるTOC情報がCPU224に送られる。

【0058】当該CPU224は、上記TOCデコーダ219からのデータより、前記鍵格納場所情報を取り出す。CPU224は、当該鍵格納場所情報に基づいて、鍵情報を後述するようにして取り出し、この鍵情報をデジタル信号処理回路220の複数の暗号鍵情報蓄積回路222<sub>1</sub>~222<sub>N</sub>に蓄積させる。

【0059】デジタル信号処理回路220は、複数の復号器221<sub>1</sub>~221<sub>N</sub>と複数の暗号鍵情報蓄積回路222<sub>1</sub>~222<sub>N</sub>を有してなるものであり、各復号器221<sub>1</sub>~221<sub>N</sub>は、上記図1の構成のセクタ化回路13~同期付加回路18までの構成に対応する逆処理を行うものである。すなわち、前述したように、これら回路13~18の少なくとも1つ、好ましくは2以上で、鍵情報を用いた暗号化処理が施されたときに、当該デジタル信号処理回路220では、これら回路13~18のうち暗号化処理に関わった回路に対応する復号器に対して、それぞれ暗号鍵情報蓄積回路222<sub>1</sub>~222<sub>N</sub>に蓄積した鍵情報を用いて当該暗号化を解くようにする。

【0060】より具体的に説明すると、デジタル信号処理回路220は、図17に示すような構成を復号器2



211~221Nに対応して設けてなるものであり、この図17の端子113に上記2値化回路213からの出力データが供給される。この図17において、同期分離回路114では、上記図1の同期付加回路18で付加された同期信号の分離が行われる。同期分離回路114からのデジタル信号は、復調回路115に送られて、上記図1の変調回路17の変調を復調する処理が行われる。具体的には、16チャンネルビットを8ビットのデータに変換するような処理である。復調回路115からのデジタルデータは、誤り訂正復号化回路116に送られて、図1の誤り訂正符号化回路16での符号化の逆処理としての復号化処理が施される。以下、セクタ分解回路117によりセクタに分解され、ヘッダ分離回路118により各セクタの先頭部分のヘッダが分離される。これらのセクタ分解回路117及びヘッダ分離回路118は、上記図1のセクタ化回路13及びヘッダ付加回路15に対応するものである。次に、デスクランブル処理回路119により、上記図1のスクランブル処理回路14におけるスクランブル処理の逆処理としてのデスクランブル処理が施され、この出力データが端子120から出力されて、図16の出力端子223に送られる。

【0061】ここで、前述したように、記録時に図1のセクタ化回路13にて暗号化処理が施されている場合には、セクタ分解回路117にて暗号化の際の鍵情報を用いた暗号の復号化処理が行われ、以下同様に、図1のスクランブル処理回路14での暗号化処理に対応してデスクランブル処理回路119での暗号復号化処理が、図1のヘッダ付加回路15での暗号化処理に対応してヘッダ分離回路118での暗号復号化処理が、図1の誤り訂正符号化回路16での暗号化処理に対応して誤り訂正復号化回路116での暗号復号化処理が、図1の変調回路17での暗号化処理に対応して復調回路115での暗号復号化処理が、さらに図1の同期付加回路18での暗号化処理に対応して同期分離回路114での暗号復号化処理が、それぞれ行われるようになっている。

【0062】ところで、本発明の再生装置のCPU224は、上述したように、上記TOCデコーダ219から供給された鍵格納場所情報に基づいて、実際に鍵情報が格納されている位置を求め、当該鍵格納場所情報に対応する場所に格納されている鍵情報を取り出し、当該取り出した鍵情報を、上記各復号器221~221Nに対応する暗号鍵情報蓄積回路222~222Nに蓄積させ、当該蓄積した鍵情報を用いて上記復号処理を行うようにしている。

【0063】このようなことを行うため、本発明では、図18に示すようなデータ構造の鍵格納場所情報KP1~KP<sub>N</sub>を、デジタル信号処理回路220内のそれぞれの復号器221~221N毎に用意し、当該鍵格納場所情報KP1~KP<sub>N</sub>が前記記録媒体101のTOC領域に配置されている。

【0064】ここで、上記各鍵格納場所情報KP1~KP<sub>N</sub>は、この図18に示すように、セクタアドレス情報とオフセット情報とバイト数情報と属性情報とからなるものである。すなわち、これら各鍵格納場所情報KP1~KP<sub>N</sub>は、ある復号器で暗号化を解くために必要な暗号鍵情報CKが、セクタアドレス情報にて示されるセクタ内において、オフセット情報にて示される位置（先頭バイトからオフセット情報にて示される位置のバイト）からバイト数情報にて示される長さのバイト分に納められていることを示している。なお、属性情報としては、復号器221~221Nの使用の有無や、その他の情報を納めることができる。

【0065】次に、上記鍵格納場所情報テーブルを用いた場合の図16の再生装置における復号処理の流れを以下に説明する。

【0066】図16の再生装置は、ディスク状記録媒体101が交換される度に、全ての復号器221~221N、暗号化鍵情報蓄積装置222~222Nをリセットすると共に、ディスク状記録媒体101の全セクタアドレスをアクセス可能なモードに設定する。

【0067】次に、再生装置は、ディスク状記録媒体101のTOC領域から上記鍵格納場所情報KP1~KP<sub>N</sub>を読み出し、これら鍵格納場所情報KP1~KP<sub>N</sub>において各々の復号器221~221Nのエントリに示された属性情報により、該当する復号器の使用の有無を判断する。ここで、もしもその復号器が使用される場合には、鍵格納場所としてセクタアドレス情報に示されているセクタの内容を読み出して（特殊なアドレスが書かれている場合については後述する）、さらにこのセクタから上記オフセット情報とバイト数情報にて示される範囲の情報を読み出して暗号鍵情報を取り出した後、その暗号鍵情報を暗号鍵情報蓄積手段222に蓄積すると共に復号器221にセットして暗号化を解く（すなわち平文化する）ための準備を完了する。これをすべての復号器221~221Nについて繰り返す。

【0068】その後、再生装置は、ユーザのアクセス領域制限モードに移行する。

【0069】次に、再生装置はユーザのコマンドを受け付け、これに応じてユーザデータを読み出し、当該ユーザデータに施されている暗号化を上記暗号鍵情報蓄積手段222に蓄積した暗号鍵情報に基づいて解く。

【0070】以下に、上記鍵情報とその格納場所、及び鍵格納場所情報について説明する。

【0071】ここで、セクタアドレス情報にて示されるセクタアドレスとしては、ディスク状記録媒体101上の全てのセクタを対象にできるので、例えばセクタアドレス情報が4バイトの2の補数形式で表されているとし、例えばTOC領域のようなシステムで使用する領域が(0ffffffffffh)にあるとしたとき、その中に収められている本来は別の目的、例えば製造履歴の記

録などに利用するために書き込まれている認識情報を暗号鍵情報として指定することができることになる。例えば、製造履歴情報がTOC領域のセクタ内の先頭から160バイト目の16バイト分に記録されているとしたとき、オフセット情報=160バイト目とし、バイト数情報=16バイトとすれば、これらにより上記製造履歴の認識情報を指定することができる。

【0072】また、例えば、セクタアドレスとして(0ffffffffff0h)のような負の値を設定して、ユーザがアクセス不可能な領域(この場合、例えばリードインエリア等)に書かれた暗号鍵情報を指定することで、暗号鍵をユーザから隠すことができるようになる。

【0073】さらに例えば上記ディスク状記録媒体101が複数の記録層を持つものであるとしたとき、当該記録媒体101上のデータ記録層とは別の記録層のセクタアドレスが例えば(7fffffffh)から減少していくように定められているような場合において、セクタアドレス情報として(7fffffffh)を指定することで、当該記録媒体101上のデータ記録層とは別の記録層の最初のセクタに収められた暗号鍵情報を指定することができる。

【0074】また、セクタアドレス情報に特殊なアドレスが書かれている例として、ディスク状記録媒体101上に存在しないセクタアドレスの番号、例えば(90000000h)から(0effffffffh)等を下記に挙げるような情報それぞれに割り当てることにより、セクタアドレスという統一的な表現で種々の情報を暗号鍵情報として取り扱うことができる。

【0075】この場合は、通常のセクタから鍵情報を読み出す構成の代わりに、媒体上の別の記録形式、例えばバーコード、ウォブリング、紫外線等で書かれた情報や、図16に示す装置内のEEPROM225などに記録されている記録/再生装置固有の識別情報や装置の出荷先の地域を表す仕向け情報(Regional Code)や、装置に接続若しくは内蔵されているICカードやいわゆるPCMCIA(Personal Computer Memory Card International Association)などの情報蓄積装置226に蓄積された情報や、通信インターフェイス227を介するモデム/LANなどの通信装置から供給される情報や、キーボード228やリモコン送信装置232からリモコン受信手段229により受信した外部装置から供給される情報等を、識別情報として取り出すようにする。

【0076】ここで、例えば鍵格納場所情報を読み出したとき、例えばディスク状記録媒体101の盤面上に記録されたバーコードBCに収められた情報を鍵情報とすることが、上記特殊なセクタアドレス(90000000h)としてセクタアドレス情報に指定されていた場合、通常の読み出し装置とは独立に設けられているバーコード読み取り装置210を動作させ、この読み取り装置210からの情報をバーコード解読装置233にて解

読し、この解読した情報をCPU224に送るようにすれば、上述同様に鍵情報を復号器に設定することができる。

【0077】なお、キーボード228やリモコン送信装置232及びリモコン受信手段229のような人と対話的に入力を行うような装置が、暗号鍵格納場所として指定されたときには、装置に内蔵または接続された表示回路230及びディスプレイ装置231などを使って、上記操作する人に対して暗号鍵の入力を促す工程が、鍵情報の読み取り工程の手前に必要となる。

【0078】このような特殊セクタアドレスを使う場合には、鍵格納場所情報のオフセット情報やバイト数情報に対しては、それぞれの情報や装置固有の意味を持たせることにより、装置間の相違点を吸収することができる。例えば、暗号鍵情報をモデムから読み込むような指定が行われた場合、暗号鍵情報の配布会社の電話番号の指定に、オフセット情報を使う例が考えられる。

【0079】また、暗号鍵情報を用いて暗号化を解く場合の他の例としては、セクタ単位で復号できる復号器Aと、媒体単位で復号できる復号器Bがあった場合、例えば上記セクタ単位の復号器Aにて暗号鍵を読み出した後、当該復号器Aに暗号鍵を設定する動作を復号器Bの暗号鍵を取り出す動作の前に行うことにより、復号器Bの暗号鍵の隠匿性をより増すことができる。

【0080】なお、上述の説明では、記録装置で複数の暗号化処理を行い、それに対応して再生装置に複数の復号器を設ける例を挙げているが、本発明は基本的には一つの暗号化処理とそれに対応する一つの復号器を設けるものであっても適用できることは言うまでもない。

【0081】上述したように、本発明の上記構成例によれば、暗号鍵情報の配置場所をその装置の持つ復号器に応じて用意(必要ならば複数用意)し、それぞれに配置場所を指し示すポインタ(鍵格納場所情報)を媒体上に記録することにより、暗号鍵情報の配置場所を媒体上の任意の位置に柔軟に指定することが可能となり、例えばユーザアクセス不能な場所を指定することにより暗号鍵情報の隠匿性を高めることができる。また、すでに物理フォーマットで規定されている任意の認識情報を指定したり、媒体の物理的特徴(例えば記録面を複数もつ媒体の別の記録層)を指定することにより、不法な複製に対する抑止力を高めたり、複数の暗号鍵を一つのセクタ内に一まとめにしておくので、多数の暗号鍵に対して高速アクセスが可能となる。

【0082】また、鍵格納場所情報の指す鍵情報は、媒体上の通常の読み出し手段で読み出されるデータ領域のみならず、別の記録方法で媒体上に記録された情報を指定することも可能である。さらに、鍵格納場所情報が指す鍵情報は、媒体上のみならず、記録再生装置に付随する論理デバイスも指定できるので、記録再生装置の内部情報(認識番号など)を指定したり外部装置からの暗号

10

20

30

40

50

鍵の入力にも対応できる。

【0083】また、鍵情報の組み合わせは、媒体の原盤毎に変更可能なので、再生装置におけるそれぞれの復号器の特性を生かして、鍵情報の一部分しか使わないなど、原盤作製者の意向にそった媒体の作製が容易に行える。

【0084】もちろんこの配置方法は、一般的な暗号化手法の鍵情報配置においても応用可能であることは言うまでもない。

【0085】次に、図17の各構成要素における暗号復号化処理について、説明する。

【0086】先ず、図17の同期分離回路114での暗号復号化処理は、上記図13や図14と共に説明したように、複数種類、例えば4種類の同期ワードの使い方はフレーム構造内での各種同期ワードの使用位置が鍵情報に応じて変更され、暗号化がなされたものを、鍵情報に応じて検出することで行われる。

【0087】次に、復調回路115での暗号復号化処理は、図19に示すように、同期分離回路114から16-8変換回路131に送られて16チャンネルビットが8ビットデータに変換されたものを、上記図12のExOR回路73に対応するExOR回路132に送り、端子133からの8ビットの鍵情報との排他的論理和をとることで、図12の入力端子71に供給された8ビットデータに相当するデータが復元され、これが誤り訂正復号化回路116に送られる。

【0088】次に、誤り訂正復号化回路116では、例えば上記図10の誤り訂正符号化処理の逆処理が、図20の構成により行われる。

【0089】この図20において、上記復調回路115にて復調されたデータの170バイトあるいは170シンボルを1まとまりとして、インバータ部172aを有する再配列回路142を介し、遅延回路143を介して第1の復号器であるC1デコーダ144に送られている。このC1デコーダ144に供給される170バイトのデータの内22バイトがP、Qパリティであり、C1デコーダ144では、これらのパリティデータを用いた誤り訂正復号化が施される。C1デコーダ144からは、170バイトのデータが出力されて、遅延回路145を介して第2の復号器であるC2デコーダ146に送られ、パリティデータを用いた誤り訂正復号化が施された後、さらに遅延回路147を介して第3の復号器であるC3デコーダ148に送られる。ここで、遅延回路147及びC3デコーダ148は、上記遅延回路143及びC1デコーダ144と同様のものであり、この遅延回路とC1デコーダの組を複数組設けるようにしてもよい。このC3デコーダ148で最終的な誤り訂正復号化が施され、パリティ無しの148バイトのデータが取り出される。この148バイトのデータは、上記図10のC1エンコーダ52に入力される148バイトのデータ

に相当するものである。

【0090】そして、図10の誤り訂正符号化回路の再配列回路57内のインバータ部57aで、インバータの有無による暗号化が施されている場合には、図20の誤り訂正復号化回路の再配列回路142内のインバータ部142aにて、対応する暗号復号化を行うことが必要とされる。その他、図10と共に説明した各種暗号化処理に対応して、その暗号化を解くための逆処理となる暗号復号化が必要とされることは勿論である。

【0091】ここで、図21は、上記図11の誤り訂正符号化回路の具体的構成に対応する誤り訂正復号化回路の具体的な構成を示す図である。

【0092】この図21において、上記図11の再配列回路57内のインバータ部57aの出力側に挿入されたExOR回路群61に対応して、再配列回路142のインバータ部142aの入力側及び遅延回路143の入力側の位置に、ExOR回路群151が挿入され、図11のC1エンコーダ52の入力側に挿入されたExOR回路群66に対応して、C3デコーダ148の出力側にExOR回路群156が挿入されている。

【0093】これらのExOR回路群151、156は、上述したように、図11のExOR回路群61、66によるデータ変換をそれぞれ復号化するためのデータ変換を施すものであり、ExOR回路群151は、例えば170個の8ビットExOR回路により、またExOR回路群156は、148個の8ビットExOR回路によりそれぞれ構成されている。なお、記録側の図11の誤り訂正符号化回路のExOR回路群61で、パリティデータを除く148バイトの情報データに対して鍵情報に応じたデータ変換が施されている場合には、ExOR回路群151は148個の8ビットExOR回路により構成されることは勿論である。

【0094】この図21の端子152には、図11の端子62に供給される鍵情報に相当する170ビットの鍵情報が供給され、いわゆるDラッチ回路153を介してExOR回路群151内の170個の各ExOR回路にそれぞれ供給されている。Dラッチ回路153は、イネーブル端子154に供給された1ビットの暗号化制御信号に応じて、端子152からの170ビットの鍵情報をそのままExOR回路群151に送るか、オールゼロ、すなわち170ビットの全てを“0”とするかが切換制御される。また、ExOR回路群156については、148個のExOR回路を有し、鍵情報が図11の端子67に供給される鍵情報と同様の148ビットであること以外は、上記ExOR回路群151の場合と同様であり、端子157に供給された148ビットの鍵情報がDラッチ回路158を介してExOR回路群156内の148個のExOR回路にそれぞれ送られると共に、Dラッチ回路158はイネーブル端子159の暗号化制御信号により148ビットの鍵情報がオールゼロとするかが切換制御される。

【0095】このように、誤り訂正回路のインバータや

ExOR回路等を暗号化の鍵として使うことにより、簡易で大きな暗号化が実現できる。また、このインバータ等の数を制御することにより、絶対再生不可能な暗号化レベルのデータとか、エラー状態が悪くなると再生不可能となるデータとか、セキュリティレベルの要求に応じて対応できる。すなわち、インバータやExOR回路等の個数をコントロールすることにより、エラー状態の良いときは再生でき、悪くなると再生ができなくなるような制御も可能となり、また、エラー訂正のみでは回復不可能な絶対再生不可能状態を形成することもできる。また、暗号化の鍵としては、上記図示の例のように1箇所当たり百数十ビットもの大きなビット数となり、鍵のビット数の大きな暗号化ができるため、データセキュリティが向上する。しかも、このようなエラー訂正符号化回路やエラー訂正復号化回路を、いわゆるLSIやICチップのハードウェア内で実現することにより、一般ユーザからはアクセスが困難であり、この点でもデータセキュリティが高いものとなっている。

【0096】次に、セクタ分解回路117においては、上記図2、図3と共に説明したように、記録時に上記セクタ化回路13で偶数・奇数バイトのインターリーブによる暗号化が施されている場合に、この偶奇インターリーブを解くような逆の処理、いわゆるデインターリーブ処理を施すものである。

【0097】また、ヘッダ分離回路118においては、記録時に、上記ヘッダ付加回路15において、上記図7～図9と共に説明したような暗号化処理、すなわちセクタ同期となるデータシンクのバイトパターンの転置や、アドレス、CRCの変更がなされている場合に、これを復元するような暗号復号化処理を施すものである。

【0098】次に、図22は、デスクランブル処理回路119の具体例を示しており、端子161には、図17のヘッダ分離回路118からのデジタルデータが供給されている。この端子161からのデジタルデータは、例えば上記図4に示すような構成を有するスクランブラ163でデスクランブル処理され、出力端子164より取り出される。このスクランブラ163についての、上記図4と共に説明したような生成多項式165及びプリセット値（あるいは初期値）166を、認証機構171からの暗号の鍵情報に応じて変化させることにより、暗号復号化を行うことができる。この認証機構171では、上記ヘッダ情報167のコピー情報46の内容や、媒体固有のあるいは再生装置固有の固有識別情報172や、製造者、販売者等の共通識別情報173や、外部から与えられる外部識別情報174等により、暗号の鍵情報を生成し、この鍵情報に応じて生成多項式165やプリセット値166を制御する。

【0099】これらの各回路114～119のいずれで暗号復号化処理が必要とされるかの情報も、暗号の鍵情報となることは前述した通りである。また、暗号の鍵情報

報を所定周期、例えばセクタ周期で切り換えることができ、この切換を行うか否かや、切換周期等も鍵とすることにより、暗号化の難易度が高められる。

【0100】次に、本発明の第2の実施の形態について説明する。この第2の実施の形態は、上述した第1の実施の形態の構成を部分的に変更したものであり、全体の基本構成は、前述した図1に示す通りである。この図1の構成の各回路13～18の内の変更部分について以下説明する。

10 【0101】図1のセクタ化回路13は前述した第1の実施の形態と同様に構成すればよいが、スクランブル処理回路14については、図23に示す構成を用いている。

20 【0102】この図23に示すスクランブル処理回路14において、データ入力用の端子35には、LSB（最下位ビット）が時間的に先となる順序、いわゆるLSBファーストで、図1のセクタ化回路13からのデータが入力される。スクランブル用の15ビットのシフトレジスタ14aは、排他的論理和（ExOR）回路14bを用いて生成多項式 $x^{15}+x^4+1$ に従ったフィードバックがかけられ、15ビットのシフトレジスタ14aには、図24に示すようなプリセット値（あるいは初期値）が設定されるようになっており、図24のプリセット値の選択番号は、例えばセクタアドレスの下位側4ビットの値に対応させて、セクタ単位でプリセット値が切り換えられるようになっている。シフトレジスタ14aからの出力データと端子35からの入力データとは、ExOR回路14cにより排他的論理和がとられて、端子14dより取り出され、図1のヘッダ付加回路15に送られる。

30 【0103】ここで、上記プリセット値（初期値）を、所定の識別番号等の鍵情報に応じて変化させるようにすることができる。すなわち、上記図24のプリセット値テーブルの各プリセット値を、例えば16バイトの識別情報の各バイト値と論理演算することが挙げられる。この場合の識別情報としては、上述したような媒体固有の識別情報、製造元識別情報、販売者識別情報や、記録装置やエンコーダの固有の識別情報、媒体製造装置固有の識別情報、外部から供給される識別情報等、あるいはこれらの組み合わせや他の情報との組み合わせ等を用いることができ、また上記論理演算としては、排他的論理和（ExOR）や、論理積（AND）、論理和（OR）、シフト演算等を使用できる。

【0104】次に、この第2の実施の形態のセクタフォーマットとしては、例えば、図25に示すようなものを用いている。

50 【0105】この図25に示すように、1セクタは、1行172バイトの12行、すなわち2064バイトから成り、この中にメインデータ2048バイトを含んでいる。12行の最初の行の先頭位置には、4バイトのID（識別データ）と、2バイトのIED（IDエラー検出

符号)と、6バイトのRSV(予備)とがこの順に配置されており、最後の行の終端位置には、4バイトのEDC(エラー検出符号)が配置されている。

【0106】上記ID(識別データ)の4バイトは、図26に示すように、MSB側の最初のバイト(ビットb31~b24)はセクタ情報から成り、残りの3バイト(ビットb23~b0)はセクタ番号から成っている。セクタ情報は、MSB側から順に、1ビットのセクタフォーマットタイプ、1ビットのトラッキング方法、1ビットの反射率、1ビットの予備、2ビットのエリアタイプ、2ビットの層番号の各情報から成っている。

【0107】図1のヘッダ付加回路15では、このようなセクタフォーマットにおいて、例えば上記ID(識別データ)の内のセクタ番号の24ビットに対して、上記鍵情報に応じて例えばビット単位でのスクランブル処理である転置処理を施すことにより、暗号化を施すことができる。また、上記2バイトのIED(IDエラー検出符号)の生成多項式や、4バイトのEDC(エラー検出符号)の生成多項式等を上記鍵情報に応じて変更することによっても、あるいはこれらの情報と鍵情報とを論理演算することによっても、暗号化を施すことができる。

【0108】次に、図1の誤り訂正符号化回路16としては、図27に示すような構成の回路が用いられる。この符号化は、図28に示すような積符号あるいはブロック符号が用いられる。図27において、入力端子310には、前記図1のヘッダ付加回路15からのデータが供給され、この入力データは、第1の符号化器であるPOエンコーダ311に送られる。このPOエンコーダ311への入力データは、図28に示すように、B<sub>0,0</sub>~B<sub>191,171</sub>の172バイト×192行のデータであり、POエンコーダ311では、172列の各列192バイトのデータに対して、それぞれ16バイトずつのリード・ソロモン(RS)符号としてのRS(208,192,17)の外符号(PO)を付加している。POエンコーダ311からの出力データは、前述したような暗号化のためのデータ変換回路312を介して、インターリーブ回路313に送られてインターリーブ処理され、PIエンコーダ314に送られる。このPIエンコーダ314では、図28に示すように、上記POパリティが付加された172バイト×208行のデータの各行の172バイトのデータに対して、それぞれ10バイトずつのRS(182,172,11)の内符号(PI)を付加している。従って、このPIエンコーダ314からは、182バイト×208行のデータが出力されることになる。この出力データは、前述したような暗号化のためのデータ変換回路315を介して、出力端子316より取り出される。

【0109】ここで、データ変換回路312については、POエンコーダ311が各列毎の192バイトの入力データに対して16バイトのPOパリティを付加して208バイトのデータを出力することから、この16バ

イトのパリティに対して、あるいは208バイトのデータ全体に対して、前述したようなデータ変換を行うことにより暗号化を施すことができる。このデータ変換は、前述したように、入力される鍵情報に応じて施すようにしてもよい。また、データ変換回路315については、PIエンコーダ314が各行の172バイトのデータに対して、それぞれ10バイトずつのPIパリティを付加して182バイトのデータを出力することから、この10バイトのパリティに対して、あるいは182バイトのデータ全体に対してデータ変換を行うことにより暗号化を施すことができる。

【0110】上記データ変換は、具体的には、前記図10、図11と共に説明したように、インバータを所定位置に配設したり、ExOR回路群により鍵情報に応じて選択的にデータを反転させたり、その他、AND、OR、NAND、NOR回路群等を使用してもよい。また、8ビット単位で1ビットの鍵情報あるいは鍵データによる論理演算を行う以外にも、8ビットの情報データに対して8ビットの鍵データで論理演算を行わせてもよく、さらに、情報データの1ワードに相当する8ビットの内の各ビットに対してそれぞれAND、OR、ExOR、NAND、NOR、インバート回路を組み合わせて使用してもよい。また、AND、OR、ExOR、NAND、NOR、インバート回路を組み合わせて使用する場合には、これらの組み合わせ自体も鍵として用いることができる。また、論理演算以外に、データの位置を変える転置や、データの値を置き換える置換等も上記データ変換として使用できる。また、シフトレジスタを用いて変換したり、各種関数演算により変換する等、さまざまな暗号化手法が適用できることは勿論であり、それらを組み合わせて使用することも可能である。

【0111】誤り訂正符号化された上記182バイト×208行のデータは、行についてインターリーブされ、13行ずつ16のグループに分けられて、各グループが記録セクタに対応付けられる。1セクタは、182バイト×13行の2366バイトとなるが、これらが変調されて、図29に示すように1行当たり2つの同期コードSYが付加される。変調には、前述した第1の実施の形態と同様に8-16変換が用いられるが、1行は2つのシンクフレームに分けられ、1シンクフレームは、32チャンネルビットの同期コードSYと1456チャンネルビットのデータ部とから成っている。図29は、変調され同期付加されて得られた1セクタ分の構造を示し、この図29に示す1セクタ分の38688チャンネルビットは、変調前の2418バイトに相当する。

【0112】図29の変調出力信号には、8種類の同期コードSY<sub>0</sub>~SY<sub>7</sub>が用いられており、これらの同期コードSY<sub>0</sub>~SY<sub>7</sub>は、上記8-16変換の状態(ステート)に応じて、ステート1及び2のときが図30の(a)、ステート3及び4のときが図30の(b)の同



期パターンとなっている。

【0113】このような8種類の同期コードSY0～SY7の選択を、例えば図31に示すような回路を用いて、3ビットの鍵情報に応じて変更することにより、暗号化が行える。すなわち、上記8種類の同期コードSY0～SY7を指定する3ビットデータ321の各ビットと、上記3ビットの鍵情報322の各ビットとを、3つのExOR回路323、324、325によりそれぞれ排他的論理和をとることにより、新たな同期コード指定データ326とする。これにより、上記フレーム構造における同期コードの使い方あるいはフレーム構造内での各種同期コードの使用位置が変更され、暗号化がなされることになる。勿論、その3ビットに対して鍵情報に応じてデータを転置したり、置換したり、シフトレジスタにより変換したりできる。また、これは関数変換でもかまわない。

【0114】以上説明した本発明の第2の実施の形態における効果も、前述した第1の実施の形態の場合と同様である。

【0115】次に、上述した本発明の第2の実施の形態の記録側の構成に対して、再生側の基本構成は、前記図17と同様であり、上記第2の実施の形態に示した各部の変更箇所に対応して変更された逆処理がそれぞれ施される。例えば、上記図27に示す誤り訂正符号化に対する逆処理は、図32のような構成の誤り訂正復号化回路により実現できる。

【0116】すなわち、この図32において、入力端子330には前記図17の復調回路115からの出力信号であり、上記図27の出力端子316からの出力に相当する上記図28の積符号の182バイト×208行のデータが供給されている。この入力端子330からのデータは、データ逆変換回路331に送られて、上記図27のデータ変換回路315の逆処理が行われる。データ逆変換回路331からの出力データは、PI（内符号）デコーダ332に送られて、上記図27のPIエンコーダ314の逆処理としての復号化処理すなわちPI符号を用いた誤り訂正処理が施され、上記図28の172バイト×208行のデータとなる。PIデコーダ332からの出力データは、デインターリーブ回路333で上記インターリーブ回路313での逆処理が施され、データ逆変換回路334に送られて上記図27のデータ変換回路312の逆処理が行われた後、PO（外符号）デコーダ335に送られる。POデコーダ335では、上記図27のPOエンコーダ311の逆処理としての復号化処理すなわちPO符号を用いた誤り訂正処理が施され、図28の元の172バイト×192行のデータが出力端子336を介して取り出される。上記図27のデータ変換回路312、315でのデータ変換の際に鍵情報を用いる場合には、各端子318、319にそれぞれ供給した鍵情報を、図32のデータ逆変換回路334、331の各

端子339、338にそれぞれ供給して、これらの鍵情報に応じてデータ逆変換を行わせればよい。

【0117】以上説明した本発明の第2の実施の形態における効果も、前述した第1の実施の形態の場合と同様である。

【0118】なお、本発明は、上述した実施の形態のみに限定されるものではなく、例えば、データ変換としては、インバータやExORの例を示しているが、その他、ビット加算や、各種論理演算等によりデータ変換を行わせてもよいことは勿論である。また、暗号化の鍵情報に応じてデータを置換したり、転置したり、シフトレジスタを用いて変換したり、各種関数演算により変換する等、さまざまな暗号化手法が適用できることは勿論であり、それらを組み合わせて使用することも可能である。この他、本発明の要旨を逸脱しない範囲で種々の変更が可能である。

#### 【0119】

【発明の効果】本発明においては、信号記録媒体には鍵情報の場所を指示する鍵格納場所情報を記録し、信号再生の際には当該鍵格納場所情報に基づいて鍵情報を取り出すようにすることにより、鍵情報を容易に取り出せないようにしているため、不法解読や不法コピーを防止することができる。

#### 【図面の簡単な説明】

【図1】本発明の信号記録装置の一構成例を示すブロック回路図である。

【図2】セクタ化回路における偶数・奇数バイトのインターリーブを実現するための構成例を示すブロック回路図である。

【図3】偶数・奇数バイトのインターリーブを説明するための図である。

【図4】スクランブラの一例を示す回路図である。

【図5】スクランブラのプリセット値を示す図である。

【図6】生成多項式が可変のスクランブラの一例を示す図である。

【図7】セクタフォーマットの一例を示す図である。

【図8】セクタ内の同期領域での暗号化の一例を説明するための図である。

【図9】セクタ内のヘッダ領域の一例を示す図である。

【図10】誤り訂正符号化回路の一例を示す図である。

【図11】誤り訂正符号化回路の他の例を示す図である。

【図12】変調回路での暗号化処理の一例を説明するための図である。

【図13】変調信号に付加される同期ワードの具体例を示す図である。

【図14】同期付加回路での暗号化の一例を説明するための図である。

【図15】データ記録媒体の一例を示す図である。

【図16】本発明の信号再生装置の一構成例を示すブ

ック回路図である。

【図17】信号再生装置のデジタル信号処理回路の具体的構成を示すブロック回路図である。

【図18】鍵格納場所情報テーブルについて説明するための図である。

【図19】復調回路での暗号化処理の一例を説明するための図である。

【図20】誤り訂正復号化回路の一例を示す図である。

【図21】誤り訂正復号化回路の他の例を示す図である。

【図22】デスクランブル処理回路の一例を示す図である。

【図23】スクランブラの他の例を示す図である。

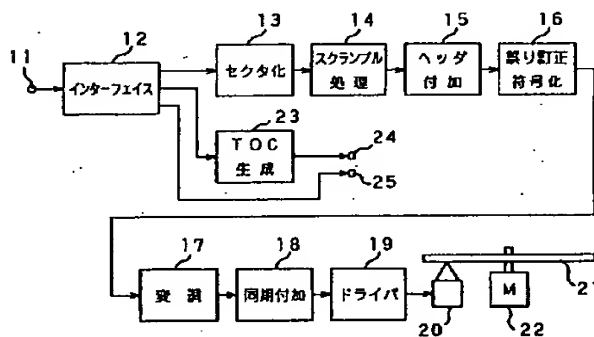
【図24】図21のスクランブラのプリセット値の一例を示す図である。

【図25】セクタフォーマットの他の例を示す図である。

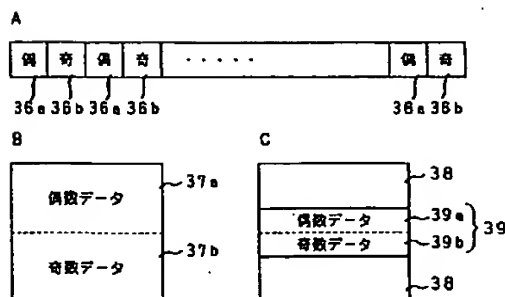
【図26】図23のセクタフォーマットにおけるセクタ内のヘッダ領域の一例を示す図である。

【図27】誤り訂正符号化回路の他の例を示すブロック図である。

【図1】



【図3】



【図28】誤り訂正符号の具体例としての積符号を示す図である。

【図29】セクタの信号フォーマットの一例を示す図である。

【図30】変調信号に付加される同期ワードの他の具体例を示す図である。

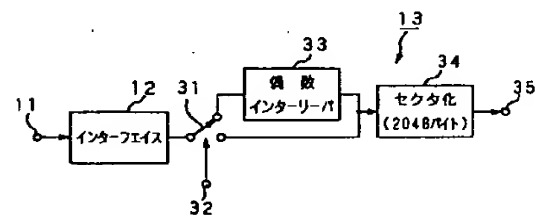
【図31】同期付加回路での暗号化の他の例を説明するための図である。

【図32】誤り訂正復号化回路の他の例を示すブロック図である。

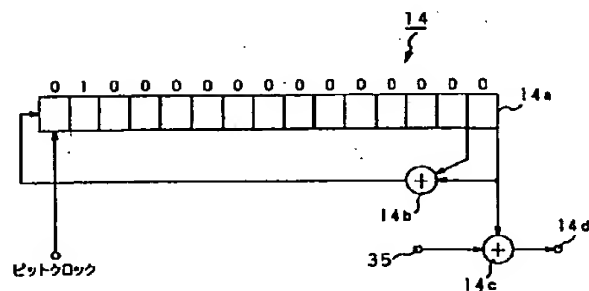
【符号の説明】

13 セクタ化回路、 14 スクランブル処理回路、  
15 ヘッダ付加回路、 16 誤り訂正符号化回路、  
17 変調回路、 18 同期付加回路、 57、  
142 再配列回路、 61、66、151、156  
ExOR回路群、 114 同期分離回路、 115 復調回路、  
116 誤り訂正復号化回路、 117 セクタ分解回路、  
118 ヘッダ分離回路、 119 デスクランブル処理回路、  
220 デジタル信号処理回路、 221<sub>1</sub>~221<sub>N</sub> 復号器、  
222<sub>1</sub>~222<sub>N</sub> 暗号鍵情報蓄積回路、 224 CPU

【図2】



【図4】

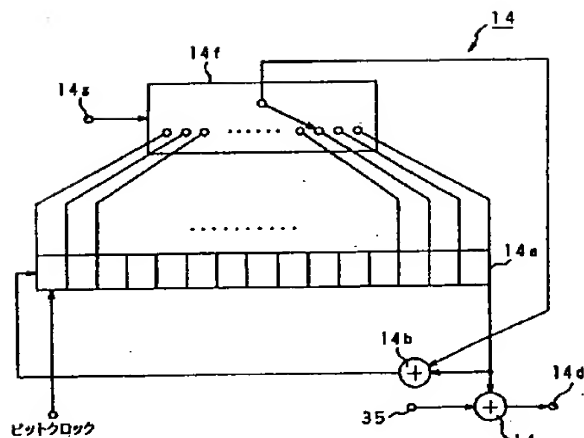




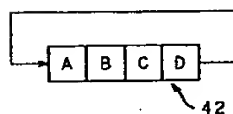
【图5】

選択番号	プリセット値	選択番号	プリセット値
0	\$0001	8	\$4080
1	\$4000	9	\$2040
2	\$2000	10	\$1020
3	\$1000	11	\$0810
4	\$0800	12	\$0408
5	\$0400	13	\$0204
6	\$0200	14	\$0102
7	\$0100	15	\$4081

【图6】



【图8】



【图7】

位置	+0	+1	+2	+3	サイズ
0	同期				4
4	ヘッダ				16
20	ユーザデータ				
2068	誤り検出符号 ( EDC )				46

サイズ合計: 2072バイト

【図9】

位置	+0	+1	+2	+3	サイズ
4	CRC		コピーガード	1	4
8	アドレス				4
12	予備				8

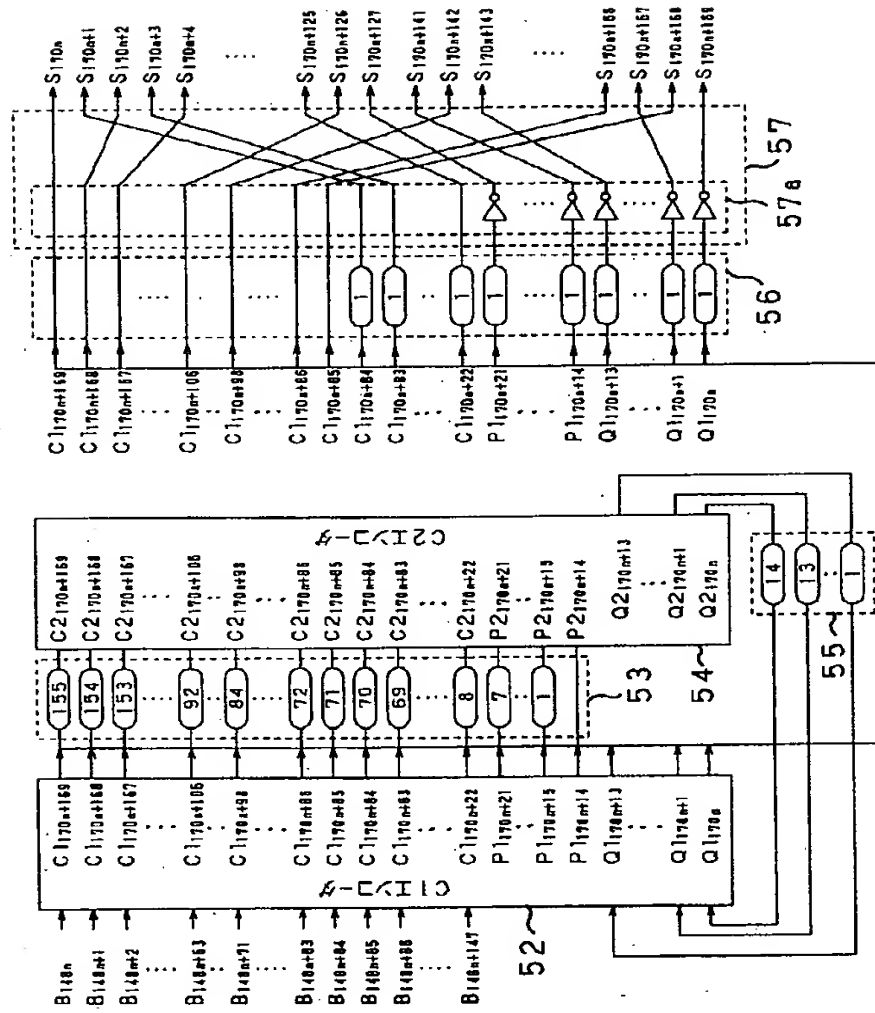
サイズ合計: 16バイト

サイズ合計：16バイト

【図 13】

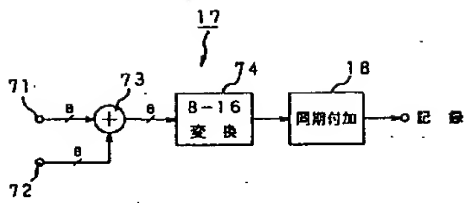
符号ワード	符号ワード						
	msb	同相パターンa		lsb	msb	同相パターンb	
S0	00010010010000000001	000000000001		10010010010000000001	000000000001		000000000001
S1	00010000010000000001	000000000001		10010000010000000001	000000000001		000000000001
S2	00000100010000000001	000000000001		10000100010000000001	000000000001		000000000001
S3	00010000010000000001	000000000001		10000100010000000001	000000000001		000000000001

【図10】

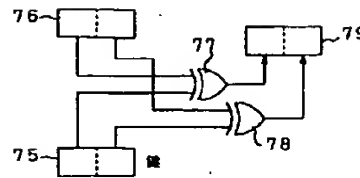




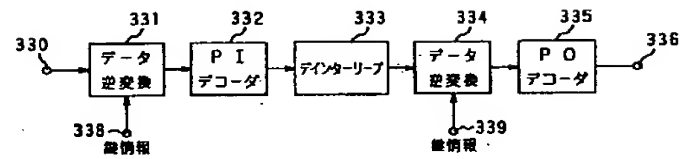
【図12】



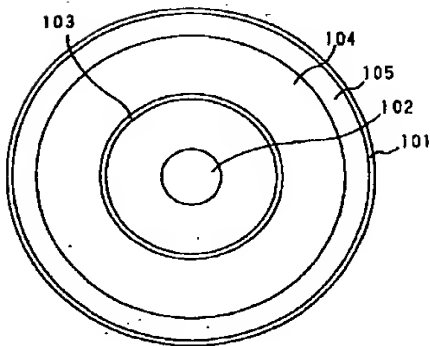
【図14】



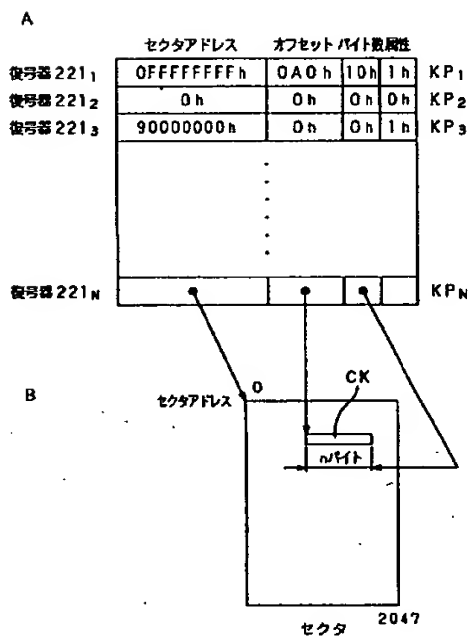
【図32】



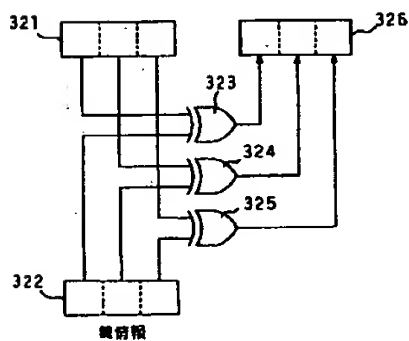
【図15】



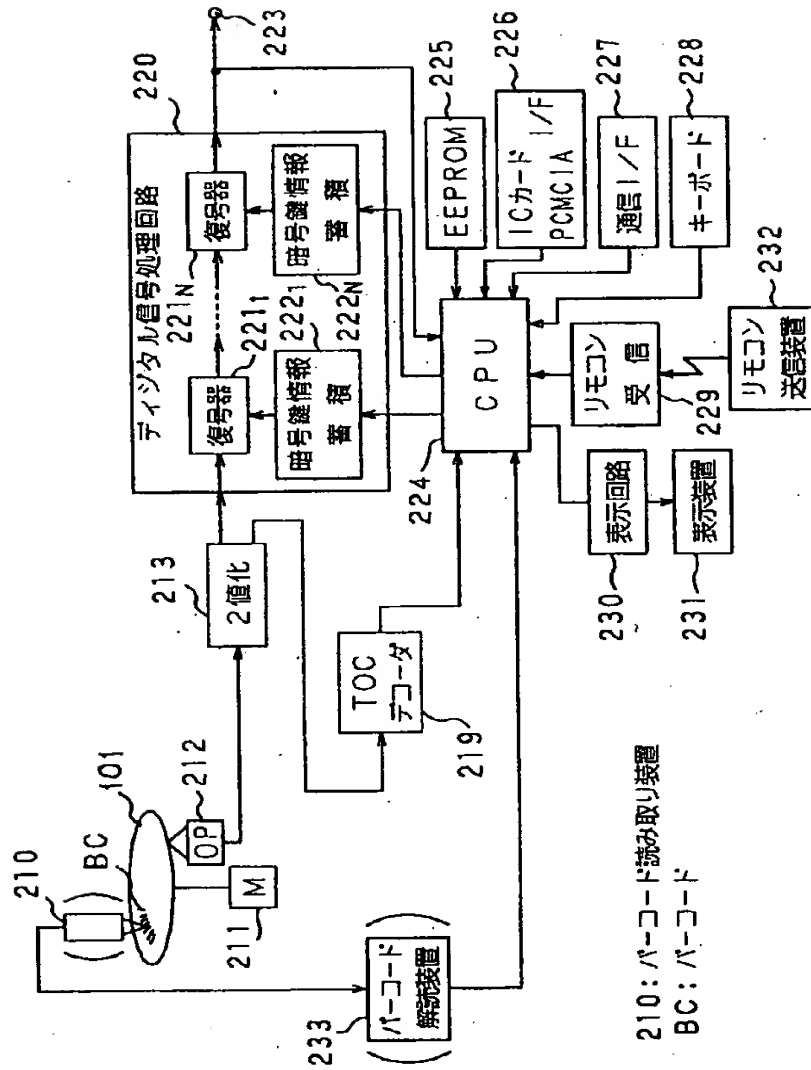
【図18】



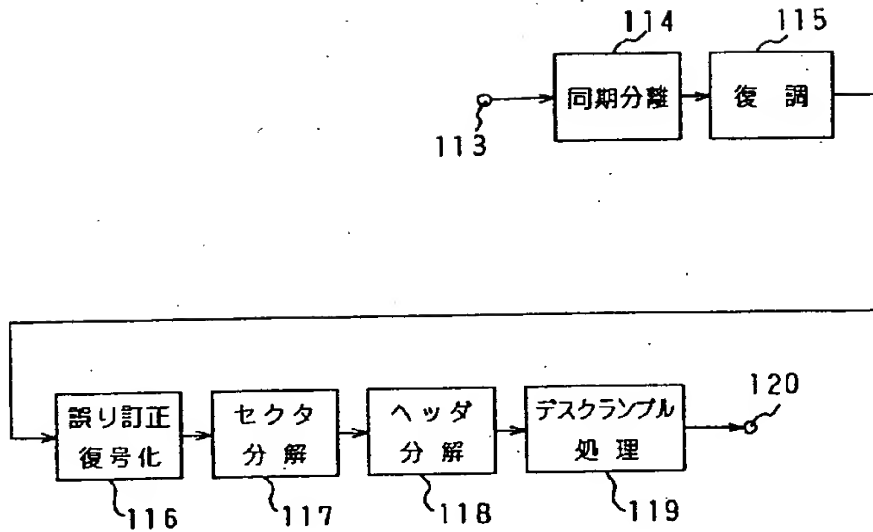
【図31】



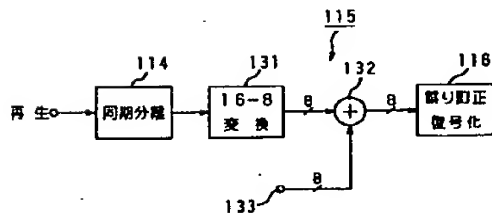
【図16】



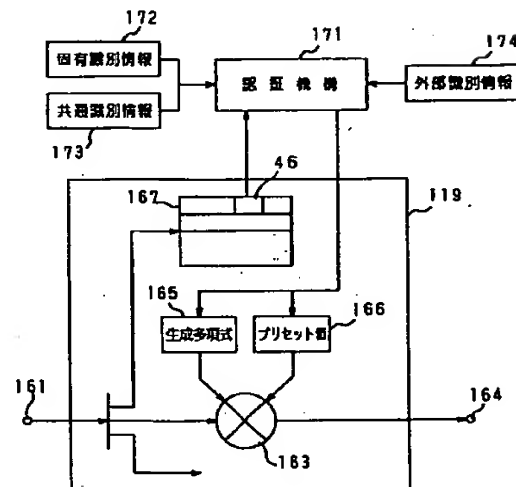
【図17】



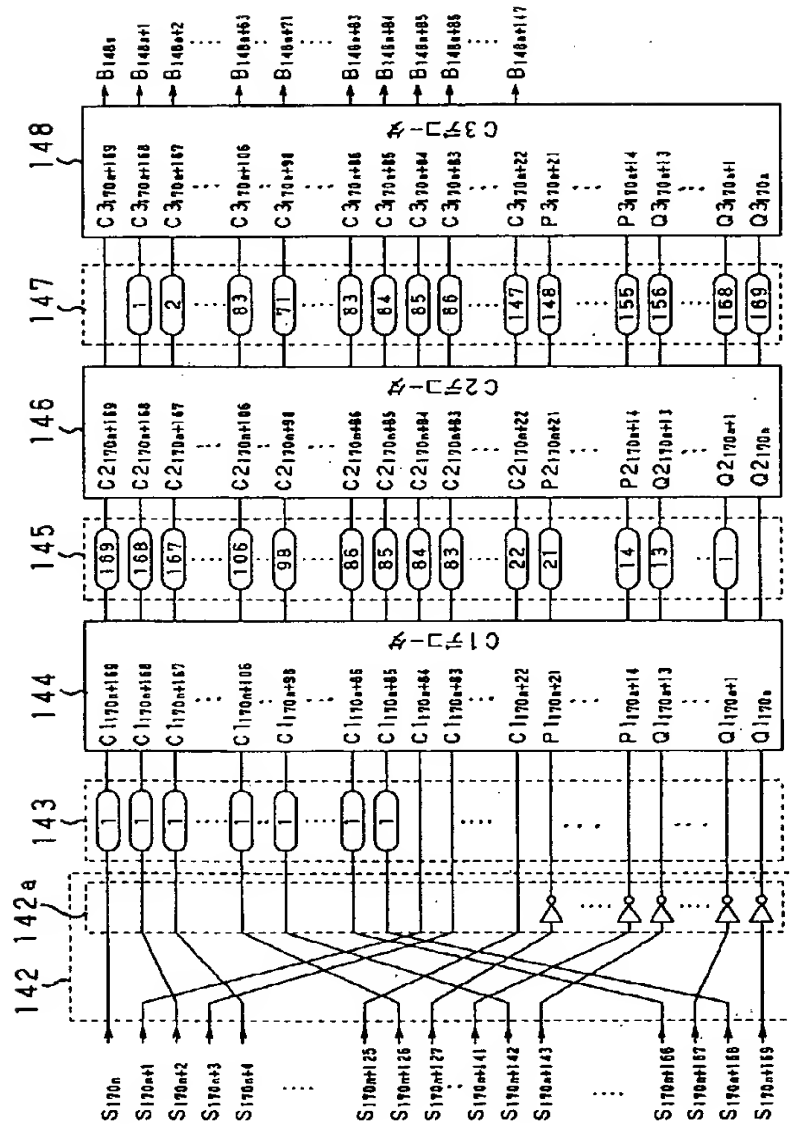
【図19】



【図22】

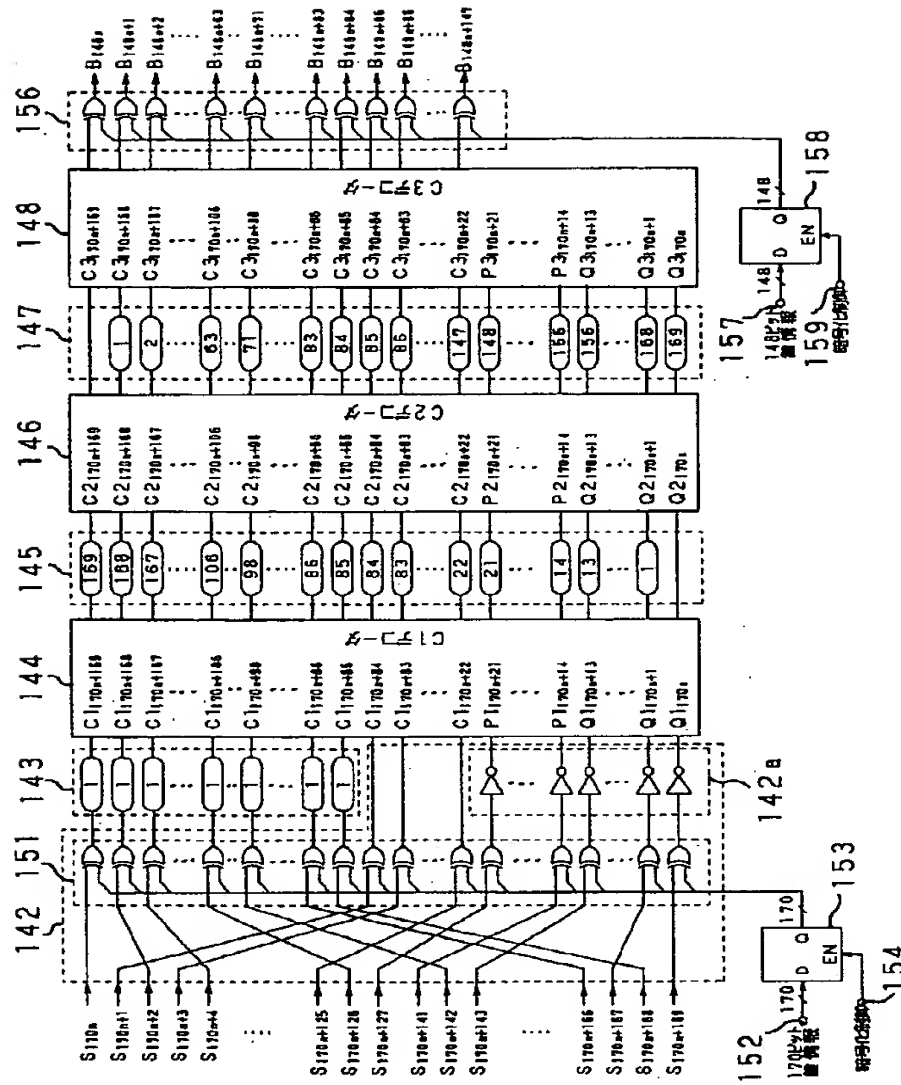


【図20】

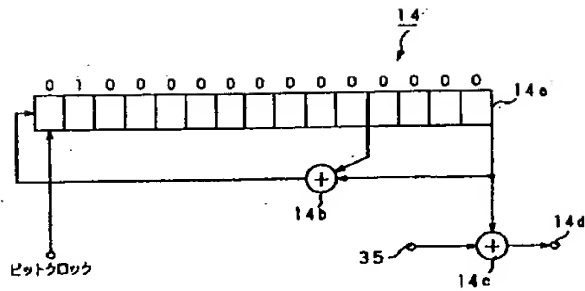




【図 2 1】



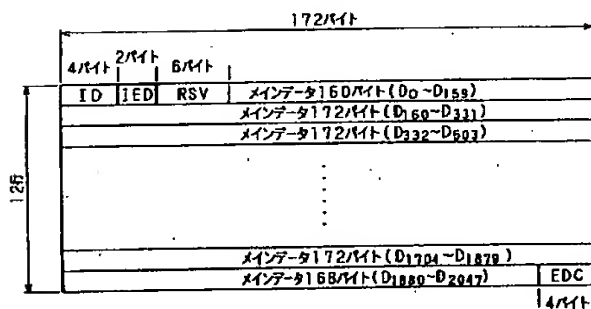
【図23】



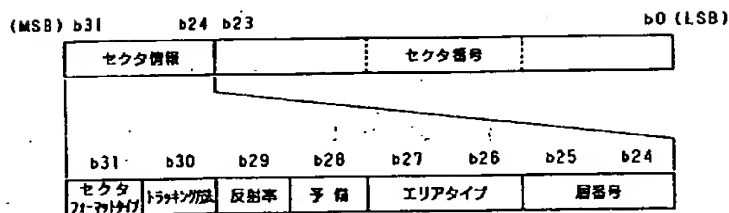
【図24】

選択番号	プリセット値	選択番号	プリセット値
0	\$0001	8	\$0010
1	\$5500	9	\$5000
2	\$0002	10	\$0020
3	\$2A00	11	\$2001
4	\$0004	12	\$0040
5	\$5400	13	\$4002
6	\$0008	14	\$0080
7	\$2800	15	\$0005

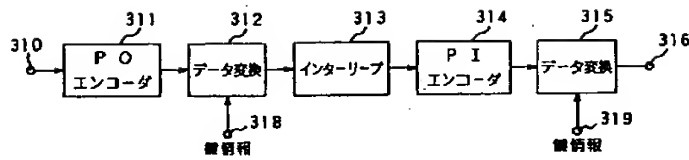
【図25】



【図26】



【図27】



【図28】

172バイト										PI 10バイト	
PO 168	B0.0	B0.1		B0.170	B0.171	B0.172		B0.181			
	B1.0	B1.1		B1.170	B1.171	B1.172		B1.181			
	B2.0	B2.1		B2.170	B2.171	B2.172		B2.181			
	B189.0	B189.1		B189.170	B189.171	B189.172		B189.181			
	B190.0	B190.1		B190.170	B190.171	B190.172		B190.181			
	B191.0	B191.1		B191.170	B191.171	B191.172		B191.181			
	B192.0	B192.1		B192.170	B192.171	B192.172		B192.181			
	B207.0	B207.1		B207.170	B207.171	B207.172		B207.181			

【図29】

32		1456		32		1456	
138	SY0			SY5			
	SY1			SY5			
	SY2			SY5			
	SY3			SY5			
	SY4			SY5			
	SY1			SY6			
	SY2			SY6			
	SY3			SY6			
	SY4			SY6			
	SY1			SY7			
	SY2			SY7			
	SY3			SY7			
	SY4			SY7			
	シンクフレーム			シンクフレーム			

【図30】

## (a) ステート1及び2

(MSB)	(LSB)	(MSB)	(LSB)
SY0=0001001001000100	000000000010001	/	000100100000100 000000000010001
SY1=0000010000000100	000000000010001	/	0000010001000100 000000000010001
SY2=0001000000000100	000000000010001	/	0001000001000100 000000000010001
SY3=0000100000000100	000000000010001	/	0000100001000100 000000000010001
SY4=0010000000000100	000000000010001	/	0010000001000100 000000000010001
SY5=0010001001000100	000000000010001	/	0010001000000100 000000000010001
SY6=0010010010000100	000000000010001	/	0010001000000100 000000000010001
SY7=0010010001000100	000000000010001	/	0010010000000100 000000000010001

## (b) ステート3及び4

(MSB)	(LSB)	(MSB)	(LSB)
SY0=1001001000000100	000000000010001	/	1001001001000100 000000000010001
SY1=1000010001000100	000000000010001	/	1000010000000100 000000000010001
SY2=1001000001000100	000000000010001	/	1001000000000100 000000000010001
SY3=1000010001000100	000000000010001	/	1000010000000100 000000000010001
SY4=1000100001000100	000000000010001	/	1000100000000100 000000000010001
SY5=1000100100000100	000000000010001	/	100010000100000100 000000000010001
SY6=1001000010000100	000000000010001	/	100100000100000100 000000000010001
SY7=1000100010000100	000000000010001	/	100010000100000100 000000000010001

フロントページの続き

(51) Int. Cl. 6	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/08			H 0 4 L 9/00	6 0 1 A

(72) 発明者 川嶋 功  
東京都品川区北品川6丁目7番35号 ソニ  
ー株式会社内